Secret Sharing

Henning Hontheim

10. März 2020

Inhaltsverzeichnis

1 Einleitung

In Public-Key-Infrastrukturen ist es oft nützlich, private Schlüssel von Teilnehmern rekonstruiren zu können. Aus Sicherheitsgründen ist es aber wichtig, dass nicht ein einzelner die Möglichkeit hat, geheime Schlüssel zu rekonstruiren. Eine Technik, um dieses Problem zu lösen, ist das Secret-Sharing, das in diesem Vortrag vorgestellt werden soll.

In Public-Key-Infrastrukturen ist es oft nützlich, private Schlüssel von Teilnehmern re- konstruieren zu können. Wenn nämlich ein Benutzer die Chipkarte mit seinem geheimen Schlüssel verliert, kann er seine verschlüsselt gespeicherten Daten nicht mehr entschlüsseln. Aus Sicherheitsgründen ist es aber wichtig, dass nicht ein einzelner die Möglichkeit hat, geheime Schlüssel zu rekonstruieren. Es ist besser, wenn bei der Rekonstruktion von privaten Schlüsseln mehrere Personen zusammenarbeiten müssen. Die können sich dann gegenseitig kontrollieren. Die Wahrscheinlichkeit sinkt, dass Unberechtigte Zugang zu geheimen Schlüsseln bekommen. In diesem Kapitel wird eine Technik vorgestellt, dieses Problem zu lösen, das Secret-Sharing. [1]

2 Beginning...

Literaturverzeichnis

[1] Buchmann, J. Einführung in die Kryptographie. *Springer-Lehrbuch* (2016).